Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 29 January 2004

Current Nationwide Threat Level is

ELEVATED

SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here

www.whitehouse.gov/homeland

Daily Overview

- Reuters reports up to a foot of snow has blanketed the New York metropolitan area, forcing officials to cancel hundreds of flights; subways, trains and buses were operating with delays. (See item 8)
- The Associated Press reports Cincinnati−based Kroger is recalling its Private Selection Roast Beef after a sample tested positive for Listeria monocytogenes in Atlanta. (See item 14)
- The Department of Homeland Security announced that its National Cyber Security Division has unveiled the National Cyber Alert System, an operational system delivering to Americans timely and actionable information to better secure their computer systems. (See item 20)
- eSecurityPlanet.com reports security researchers have released details of another spoofing flaw in Microsoft's Internet Explorer browser that could trick users into downloading malicious files; this has a moderately critical rating. (See item 21)
- eSecurityPlanet.com reports for the second time this month, Apple has released security patches to correct vulnerabilities found in several versions of its Mac OS X. (See item 26)

DHS/IAIP Update *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 28, Reuters* — **U.S. heating oil, propane supplies seen as adequate according to EIA. U.S. heating oil and propane inventories will be adequate to meet demand at least through February, even if temperatures are very cold, but prices will be higher than a year ago,** the Energy Information Administration (EIA) said on Wednesday. "Despite the frequent arctic air masses that swept over many portions of the Midwest and East Coast during January, heating fuel markets are poised to enter the last leg of the heating season with inventories that remain well positioned within their respective average ranges for this time of year," the EIA said in its weekly report on the oil market. **"Even if the cold weather persists in February and heating oil and propane inventories report sharp declines over the next several weeks, the general consensus among industry observers is that stocks are high enough that even significant draws ahead will have overall levels sufficient to meet winter requirements," EIA added.** Propane inventories in the Midwest, where propane is used predominantly for heating purposes, were 2.3 million barrels above the five−year average and four million barrels above the year−ago level. However, Americans are paying more to heat their homes with these two fuels.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_reuters.htm?SMDOCID=reuters_pma_2004_01_28_eng−reuters_pma_US−HEATING−OIL−PROPANE−SUPPLIES−SEEN−ADEQUATE−EIA&SMContentSet=0

2. *January 28, Associated Press* — **Government to test burying greenhouse gas. In hopes of developing a process that could slow global warming, the Department of Energy wants to inject carbon dioxide underground into depleted oil reservoirs after converting it into a liquid form.** The Teapot Dome project, now in the planning stages, could be one of the world's largest test sites for the method. It would store CO2 from a natural gas processing plant more than 300 miles away beneath the 10,000−acre oil field in central Wyoming. Teapot Dome is currently in its preliminary engineering and testing stages. Storage could begin by 2006 and last seven to 10 years. When a reservoir is full, the pipeline is taken out and the hole sealed up. "The objective is to keep it sealed underground forever, hundreds or thousands of years," said Dag Nummedal, director of the University of Wyoming Institute for Energy Research. The site is projected to store at least 1.6 million tons of carbon dioxide a year when fully operational. **If the project pans out, officials hope to capture CO2 from the nation's power plants, oil and gas refineries and other manufacturing facilities.**
Source: http://www.cbsnews.com/stories/2004/01/28/tech/main596500.sh tml

[Return to top]

Chemical Sector

3. *January 28, Associated Press* — **Safety board expanding probe a year after North Carolina blast.** One year after a blast killed six people at a Kinston, NC, pharmaceutical plant, federal safety investigators said Wednesday their probe would be widened to include other dust explosions. Dozens of other people were injured in the January 29, 2003, explosion at West Pharmaceutical Services Inc. West is sponsoring a service Thursday in Kinston that will commemorate the blast. **Nearly five months after the accident, investigators at the U.S.**

Chemical Safety and Hazard Investigation Board said it was caused by combustible polyethylene dust that accumulated above a suspended ceiling. But the board said the cause of ignition wasn't known. "The explosion at West Pharmaceuticals and a similar incident a few weeks later in Kentucky raise safety questions of national significance," said board chairman Carolyn Merritt. The renewed investigation will include the blast last February that killed seven workers and injured seven others at CTA Acoustics fiberglass insulation plant in Corbin, KY. A third explosion last October at an automotive parts plant in Huntington, IN, killed one man and severely burned two when aluminum dust exploded.
Source: http://www.charlotte.com/mld/observer/news/local/7818152.htm

[Return to top]

Defense Industrial Base Sector

4. *January 28, American Forces Press Service* — **DoD to transform reserve and guard. The Department of Defense (DoD) has several initiatives under way to rebalance Guard and Reserve forces, the department's top reserve affairs official said.** Thomas F. Hall, assistant secretary of defense for reserve affairs, said that Defense Secretary Donald H. Rumsfeld is interested in transforming the Guard and Reserve "not tomorrow, but today," and that the fiscal 2005 defense budget will have significant rebalancing initiatives. **Hall said the department is studying ways to improve Guard and Reserve end strength, reduce multiple mobilizations of the same units and relieve stress on the force.** Hall noted that those Guard and Reserve members called most for mobilization belong to units that specialize in mortuary, civil affairs, force protection and air traffic control. In those groups, he said, there is a need to "rebalance so that we do not mobilize those people over and over again. And we're committed to that, and that's going to be part of the rebalancing." Hall said DoD also is looking into providing more predictability for Guard and Reserve members prior to deployment. He said Guard and Reserve members "need to know up front" when they're going to mobilize and for how long.
Source: http://www.defenselink.mil/news/Jan2004/n01282004_200401283. html

5. *January 27, Air Force Print News* — **Soldiers leaving Air Force gates. A mix of airmen, civilians, contractors and new technology will replace Army National Guard military policemen now posted at Air Force bases.** The original agreement struck between the Air Force and the Army called for using the Guardsmen at base entry points for two years, enough time to find a solution to the Air Force security forces manpower shortfall, said Brig. Gen. James M. Shamess, Air Force director of security forces. However, just one year into the plan the Army faced increased requirements in 2003 to support Operation Iraqi Freedom. Their operations tempo did not decline following the end of hostilities. "We started with about 8,000 (Army National Guard) soldiers but in the second year they will only be able to provide about 6,500 on a continuing basis," General Shamess said. "We're going to fill that gap with volunteers from our Air Reserve Component, civilians and contractors." **Other options being considered for longer−term solutions include converting manpower positions in overage career fields to security forces, and making other manpower changes within the security forces career field, General Shamess said. Technological solutions will also be applied to situations where they are more efficient than posting a patrolman.**
Source: http://www.af.mil/stories/story.asp?storyID=123006461

[Return to top]

Banking and Finance Sector

6. *January 28, Government Computer News* — **To nab terrorists, DHS will plumb trade data. To detect money laundering by terrorists, drug smugglers and other criminals, the Department of Homeland Security will buy new tools to analyze trade data.** Immigration and Customs Enforcement (ICE), an arm of the department's Border and Transportation Security Directorate, plans to acquire 14 copies of software that is an improved version of the software now used by ICE to track down financial crimes. ICE analysts will use the software to detect patterns of financial activity by scanning files stowed in more than 25 databases, DHS officials said. **The data−mining tool uses a trade discrepancy feature to automate comparisons of federal trade data with information from foreign governments' databases. Trade discrepancy analysis relies on the detection of unusual patterns of exports or imports to detect criminal activity.** International terrorist organizations also have used underinvoicing and overinvoicing of traded goods to shift revenue internationally −− a practice that can be used either between companies or across subsidiaries of companies that operate in several countries. Such transfer pricing scams, which can be used to shift profits to jurisdictions with low taxes, have been outlawed by Congress and investigated by the IRS for decades.
Source: http://www.gcn.com/vol1_no1/daily−updates/24772−1.html

[Return to top]

Transportation Sector

7. *January 28, Miami Today News* — **Florida county's costs for transit security continue to mount.** Miami−Dade County has been paying a higher price for private security on its transit systems since 9/11 and the beginning of a voter−mandated transit expansion. Since 9/11, Miami−Dade Transit has added 560 hours of weekly security to its main bus−maintenance facilities, according to department documents, costing $756,000 a year and adding 336 weekly hours to Metrorail and Metromover facilities, costing $785,000 annually, according to department documents. **The 24−hour Metrorail and Metromover service that went into effect in June has meant $1.6 million a year for Wackenhut security personnel, who ride the trains at all times, according to the county's contract with Wackenhut. The 24−hour security detail went into effect in June when the round−the−clock service approved by voters November 2002 started.** When voters approved transit expansion to be paid for with a half−penny tax they also approved better security on the county's buses at the price tag of $1.1 million a year for Wackenhut guards to ride the buses and keep vandalism and crime down, wrote county Surface Transportation Manager Carlos Bonzon. For security reasons, Miami−Dade Transit and Wackenhut officials said they were unable to comment on security improvements.
Source: http://www.miamitodaynews.com/news/040129/story4.shtml

8. *January 28, Reuters* — **Snow storm cancels hundreds of New York flights. Up to a foot of snow blanketed the New York metropolitan area on Wednesday, January 28, forcing**

officials to cancel hundreds of flights and close schools in a region already chilled by freezing temperatures and above−average snowfall. While airports remained open, more than 850 flights had been canceled at the city's three major airports since the snow storm blew in on Tuesday night, airport officials said. The snow continued into Wednesday, disrupting travel plans for thousands of people. Since Tuesday night, John F. Kennedy International Airport canceled 105 flights, LaGuardia canceled 319 and Newark Liberty International Airport in neighboring New Jersey canceled 430, the Port Authority of New York and New Jersey said. The national Amtrak railway said that in the northeastern United States, it expected 80 percent out of more than 120 scheduled regional trains to operate. New York subways, trains and buses were operating with delays, officials said.
Source: http://www.reuters.com/newsArticle.jhtml?type=domesticNews&s toryID=4230499

[Return to top]

Postal and Shipping Sector

9. *January 28, DM News* — **Possible First−Class mail change. The U.S. Postal Service (USPS) is considering a broader interpretation of First−Class mail that would move many Standard mail pieces into the costlier First−Class category.** A USPS spokesman said that the issue is being discussed but that no action has been taken. Several mailers said that in the past year and a half they have been told by local acceptance clerks at postal business mail entry units that Standard mail they have sent for years now must go at the First−Class rate. Some of the mailers said that despite having letters from the USPS stating that the mail qualifies for the Standard rate, they have been told those exceptions should not have been given. A direct marketing firm, in Nashville, TN, serving banks, credit unions, and other companies, said the USPS ruled January 16 that its "Skip−A−Payment" notices could not be mailed at the Standard rate because they contain specific account data such as a loan number or payment amount. The difference between Standard and First Class for a typical bulk mailing is 8.8 cents per piece, or $88 per thousand. **For large financial mailers that often mail 10 million pieces monthly, the ruling could raise their monthly mail costs by $880,000.** The postal service also aims to have a centralized process for appeals to prevent inconsistencies that often happen in the field.
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2632 2

[Return to top]

Agriculture Sector

10. *January 28, CNN* — **Produce imports hurting U.S. farmers.** Americans' growing appetite for inexpensive vegetables year−round is feeding a steady rise in imports that is squeezing American farmers, according to a recent U.S. Department of Agriculture (USDA) study. **Fresh vegetable imports went up by seven percent in the first 10 months of 2003, a trend that may be elbowing U.S. farmers out of production, market analysts said. Fresh vegetable imports have been going up steadily, 11 percent in 2001, six percent in 2002, and seven percent last year,** said Gary Lucier, agricultural economist with the Economic Research Services branch of the USDA. Last year, California asparagus farmers had to plow under whole fields, because the prices they would get wouldn't cover the expense of harvest. In 1990, 30

percent of all asparagus consumed in the U.S. was foreign; now 65 percent comes from abroad. In 1999, there were about 36,000 acres of asparagus growing in California. Now there are 24,000. Tomato farmers also are pinched, with year−round imports from Mexico and from Canada's greenhouses. **If this trend continues, the United States may find itself relinquishing control over a large part of the produce that feeds the nation, farmers said.**
Source: http://edition.cnn.com/2004/US/West/01/28/foreign.veggies.ap /

11. *January 28, Voice of America* — **Asian countries consider monitoring network. Asian governments battling an epidemic of bird flu among their chicken flocks are considering creating a regional network to monitor livestock health.** The announcement came at the end of an emergency ministerial meeting in Thailand aimed at containing the spreading virus. **Thailand's Foreign Minister Surakiart Sathirathai said the proposed veterinary surveillance network would provide an early warning system for possible region−wide epidemics.** The meeting in Bangkok comes amid a rapidly spreading epidemic of bird flu. The disease has killed millions of chickens, and forced governments to cull millions more, causing severe hardship to the poultry industry. Wednesday's meeting included the 10 Asian countries with confirmed bird flu outbreaks, as well as Singapore, Hong Kong, the United States, and European Union.
Source: http://www.voanews.com/article.cfm?objectID=3AAAF019−04BD−4D 1D−9F369EE3A5C17FE4

12. *January 26, Reuters* — **USDA ends quarantine on five herds. The U.S. Department of Agriculture (USDA) has removed hold orders on five cattle herds being investigated as part of the first U.S. case of mad cow disease,** Chief USDA Veterinary Officer Ron DeHaven said Monday. DeHaven said the herds were in Mabton, Mattawa, Sunnyside, and Connole, WA, and Boardman, OR. It was safe to remove quarantine orders, DeHaven said, because mad cow disease is not contagious and authorities have killed animals in those herds that might be linked to the Holstein cow found with mad cow disease. Officials say 81 head entered the U.S. at the same time as the Holstein.
Source: http://www.forbes.com/markets/newswire/2004/01/26/rtr1227462 .html

[Return to top]

Food Sector

13. *January 28, USAgNet* — **All exporters to U.S. adopt mad cow rule. All countries exporting beef to the U.S. have banned sick or injured cattle from their beef supply, as requested by Washington, to prevent the spread of mad cow disease,** U.S. Department of Agriculture (USDA) Secretary Ann Veneman said on Tuesday. The USDA banned all "downer" cattle, those unable to walk because of broken bones, disease, or sickness, from being processed into human food, after the first U.S. case of mad cow disease was found late last month in a Washington state dairy cow. The department sent letters to Brazil, Argentina, Australia, and seven other beef exporting nations earlier this month, saying exports would be blocked if nations did not comply with the new rules. Of the more than 35 million cattle slaughtered in the U.S. each year, about 200,000 are downer cattle, the USDA said.
Source: http://www.usagnet.com/story−national.cfm?Id=95&yr=2004

14. *January 28, Associated Press* — **Roast beef recalled.** The Cincinnati−based Kroger company is recalling a brand of roast beef after a sample tested positive for a potentially lethal bacteria. **The company recalled the Private Selection Roast Beef Tuesday after a sample taken from a Kroger deli service counter in Atlanta by the Georgia Department of Agriculture tested positive for Listeria monocytogenes.** Listeria monocytogenes can cause short−term symptoms including high fever, severe headache, stiffness, nausea, abdominal pain, and diarrhea. The infection may be more serious or even fatal among young children, frail or elderly people, or others with weakened immune systems. The company says in a statement it has not received any reports of illnesses from customers.
Source: http://www.wsbtv.com/news/2798677/detail.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

15. *January 28, New Zealand Herald* — **Bird flu killing most of those who catch it. The Asian bird flu is killing three out of every four people who catch it, says a New Zealand virus expert at the World Health Organization (WHO).** Christchurch virologist Lance Jennings, who is fighting the outbreak with the WHO in the Philippines, said the death rate was high. "Nearly everyone who has been identified with the virus has died." Six out of eight people in Vietnam and two out of three in Thailand had died. **But the WHO was not sure of the exact death rate because it was not clear how many people had caught the virus.** Jennings said evidence from Vietnam suggested children were most at risk, since they were the main people catching the virus. The virus was therefore different to the H5N1 strain that struck Hong Kong in 1997, affecting people of all ages. Scientists have found small differences between the two viruses' amino acids.
Source: http://www.nzherald.co.nz/storydisplay.cfm?storyID=3546243&thesection=news&thesubsection=general

16. *January 27, Infectious Diseases Society of America* — **Researchers add new drug prophylactic option against flu.** Researchers examined the common influenza season scenario of a household in which a family member is infected with influenza virus. **They found that when the family member with influenza was treated with the antiviral drug oseltamivir, post−exposure oseltamivir prophylaxis of all other family members significantly reduced the frequency of virus transmission and illness in the household.** Because households are important sites of influenza virus transmission, these results have implications for the management of influenza outbreaks in the community. The prospective, open−label, randomized study was conducted in multiple centers in Europe and North America by Frederick G. Hayden of the University of Virginia and colleagues. They studied a total of 277 households with a suspected influenza introduction during the 2000−2001 season. Oseltamivir use was not associated with transmission of drug−resistant virus, which had been a problem with some

other antiviral drugs, the M2 protein inhibitors amantadine and rimantadine, when used for treatment and prophylaxis of influenza. However, early occurrence of illness in this study indicated that the treatment must be initiated quickly for optimal protection.
Source: [http://www.eurekalert.org/pub_releases/2004−01/idso−ran01270 4.php](http://www.eurekalert.org/pub_releases/2004-01/idso-ran012704.php)

17. *January 27, Washington Post* — **Strategy on bird flu has human risks. UN officials have pressed countries in the region to accelerate their culling of chickens but say the contact between poultry and the people killing them poses a risk by creating more chances for avian influenza to hijack genes from ordinary human flu.** While urging Asian governments to follow strict guidelines in slaughtering poultry, including the use of protective garb and disinfectant, UN officials acknowledge that adherence has been spotty. In Thailand, many of the estimated 3,000 soldiers and laborers conducting the slaughter now wear masks, caps, gloves, and boots. But few are supplied with the goggles that international health officials say are needed to prevent infected droplets from getting in their eyes. **About 15,000 people are involved in killing chickens in Vietnam, and UN officials say they suspect that many of them have little or no protective gear because the country is so strapped for resources.** The disclosure Tuesday by government officials in Laos that avian flu had been confirmed in chickens there is particularly troubling because of the poor condition of its public health system, according to Peter Cordingley, a regional World Health Organization spokesman. **Health officials have expressed concern about whether Laos and other developing countries have the expertise and equipment to safely contain the disease.**
Source: [http://www.washingtonpost.com/wp−dyn/articles/A52595−2004Jan 27.html](http://www.washingtonpost.com/wp-dyn/articles/A52595-2004Jan27.html)

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

18. *January 28, Government Technology* — **Miami Beach police department deploys Florida's first metro−scale Wi−Fi network for law enforcement.** The North Miami Beach Police Department (NMBPD) announced yesterday, January 27, that it has further enhanced its leadership position in public−safety innovation by deploying Florida's first metro−scale Wi−Fi network for law enforcement. **The equipment, based on the 802.11 standard, or Wi−Fi, enables NMBPD officers in the field access to applications previously unavailable outside of police headquarters. The equipment provides in−vehicle access to such applications as computer−aided dispatch, local records systems for outstanding wants and warrants, as well as state and national criminal justice information systems.** NMBPD is currently using the network in several square blocks centered around the central police headquarters. Plans to expand the coverage area are under way, pending approval from the North Miami Beach City Council. The expanded network will eventually cover the entire city core of North Miami Beach, an area of over five square miles.
Source: http://www.govtech.net/news/news.php?id=86364

19. *January 28, McCook Daily Gazette (NE)* — **Statewide radio system outlined.** Col. Tom Nesbitt is the chairman of the Statewide Communications Alliance of Nebraska (SCAN), an effort to create "interoperability," the ability of various agencies with different types of radios to communicate quickly and effectively. **Under the plan, all public safety agencies, no matter what type of radio they use, would eventually be able to tie into a "trunk" enabling them to communicate with other agencies in their area, and, using the Internet, to agencies across the state, if need be.** Project manager Curt Beck, a technical consultant, said that while the system would initially interface with whatever radio system local agencies currently use, they would eventually be expected to "migrate" to 800 mhz frequency systems. Using up to 50 cents per electric bill per customer in Nebraska, SCAN will establish the infrastructure to make the new system function. Meanwhile, McCook Police Chief Ike Brown said Red Willow County essentially achieved interoperability in 1997, when he and Red Willow County Sheriff Gene Mahon persuaded the Nebraska State Patrol to monitor local frequencies, which are also used or monitored by local public safety personnel.
Source: http://www.mccookgazette.com/story/1060789.html

[Return to top]

Information and Telecommunications Sector

20. *January 29, Department of Homeland Security* — **DHS unveils National Cyber Alert System. The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) unveiled the National Cyber Alert System Wednesday, January 28. The system will deliver timely and actionable information to Americans to help them better secure their computer systems.** As part of this program, DHS is making available a series of information products targeted for home users and technical experts in businesses and government agencies. **These e−mail products will provide timely information on computer security vulnerabilities, potential impact, and action required to mitigate threats, as well as PC security "best practices" and "how to" guidance.** "The President's National Strategy to Secure Cyberspace provides a framework for the public and private sectors to work together to secure cyberspace," said Frank Libutti, Under Secretary of Homeland Security for Information Analysis and Infrastructure Protection. The National Cyber Alert System is America's first coordinated national cyber security system for identifying, analyzing, and prioritizing emerging vulnerabilities and threats. All information products are available on a free subscription basis and are delivered via push e−mail. Home users can also access Cyber Security Tips and Cyber Security Alerts from US−CERT affiliates including StaySafe Online (www.staysafeonline.info). **For more information visit:** http://www.us−cert.gov
Source: http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0337.xml

21. *January 28, eSecurityPlanet.com* — **New IE download spoof found. Security researchers on Wednesday, January 28, released details of yet another spoofing flaw in Microsoft's Internet Explorer (IE) browser that could trick users into downloading malicious files. The latest IE bug, which carries a "moderately critical" rating from tech security consulting firm Secunia, could allow malicious Web sites to spoof the file extension of downloadable files.** Typically, an attacker could embed a CLS ID in a file name to fool users into opening malicious files as "trusted" file types. The latest IE flaw affects IE version 6. **As a**

workaround, IE users are urged to avoid using the "open file" option when downloading a file. Instead, IE users are urged to save files to a folder as this reveals the suspicious filename. Microsoft has confirmed the development of patches for several known IE vulnerabilities but the complicated testing process had led to a delay in the release of fixes. Two of the more serious IE flaws that remain unpatched include a URL spoofing bug that could be used by "phishers" to trick unsuspecting surfers into give up sensitive information, including credit card and social security numbers.
Source: http://www.esecurityplanet.com/trends/article.php/3304951

22. *January 28, CNET News.com* — **Anti−virus feature creates a burden. A common anti−virus feature that automatically replies to e−mails infected with a virus −− to inform the senders that they are infected −− is obsolete and should be disabled, because it creates almost as much trouble as the virus itself, according to security experts.** When an anti−virus application detects malware in an e−mail, such as the recent MyDoom worm, it can automatically reply to senders of messages to inform them that they have been infected. However, **virtually all modern e−mail viruses disguise the original senders' addresses by spoofing the "to" field with stolen, but valid, e−mail addresses. This means that users receive e−mails telling them that they are infected when they are not, resulting in significant quantities of unnecessary traffic.** Jay Heiser, chief analyst at TruSecure, agreed. "This technique was useful back in the days before people spoofed e−mail addresses, but it is not something that I would encourage right now. The lines are being clogged up with e−mails flying around, not only from the virus, but also from end users that are concerned they have got the virus when they don't." Heiser believes that the **autonotification feature may have worked as an incentive for virus writers to use e−mail spoofing to give their viruses more time to infect users. Experts urge administrators to disable the feature immediately.**
Source: http://news.com.com/2100−7355_3−5148995.html?tag=nefd_top

23. *January 28, Government Computer News* — **MyDoom variant starting to spread. The first variant of the virulent MyDoom worm has been discovered, just 48 hours after the worm first appeared.** The original version, W32/MyDoom.a, also known as Norvag, has since its discovery on Monday, January 26, become one of the fastest spreading e−mail worms ever, and is set to launch a denial−of−service (DoS) attack against the Website of SCO Group Inc. The company confirmed that it is already experiencing a distributed DoS attack. The new version, MyDoom.b, appears to target the Microsoft Website, and carries a few more tricks with it. **MyDoom.b blocks access to 65 sites, most of them antivirus vendors**. SCO is working with the Secret Service and the FBI. People with information should contact their local FBI office. Several security and antivirus experts have said that the new variant could be spreading via computers already infected by the original version. The back door placed on those computers could allow the machines to be used as relays for infected e−mails. “If this is the case, MyDoom.b will likely become very prevalent in the wild in just a few short hours,” Dunham said. “This does not mean that millions of computers are infected, but that millions of e−mails harboring the worm are in the wild.” **Whether these e−mails infect new machines depends on whether users open the executable attachment carrying the infection.**
Source: http://www.gcn.com/vol1_no1/daily−updates/24776−1.html

24. *January 28, eSecurityPlanet.com* — **Costs of blocking legit e−mail to soar. Marketers concerned about legitimate e−mail blocked as spam will find confirmation of their fears, a**

report finds. The costs of such blocking will nearly double, soaring to $419 million in 2008 from $230 million in 2003, according to Jupiter Research. Ironically, the percentage of wrongly blocked permission e−mail will drop from 17 percent today to just under 10 percent in 2008, researchers found. However, total spending on retention and sponsored e−mails will increase, accounting for the higher amount of money wasted on messages that are never delivered. **The report recommends that marketers use confirmed opt−in practices and says those sending millions of messages should participate in identity−based trusted and bonded sender programs. The latter measure will kick up costs to $0.005 per message from the current $0.002**, according to the report. In addition, marketers should make the permission and opt−out process easier by following four steps, according to the report. Companies should clearly state the date and time when customers opted in; they should send e−mails only for a limited period of time or make customers opt back in after a specified period of time; they should make opting out easy; and make relevancy the ultimate determinant of e−marketing frequency.
Source: http://www.esecurityplanet.com/trends/article.php/3305011

25. *January 27, Government Computer News* — **NSF launches first phase of TeraGrid. The National Science Foundation (NSF) has declared its grid−computing project, known as TeraGrid, open for business.** The first phase of the distributed computing grid switched to production mode this month, and about a dozen scientific teams are working on research programs, said Rob Pennington, interim director of the National Center for Supercomputing Applications in Illinois. **NSF wants TeraGrid to become the world's largest distributed computing infrastructure, open to researchers on a competitive basis.** Scientists, chosen by peer review last fall for the first round of research on TeraGrid, will use the distributed computers to study groundwater pollution, the dynamics of biological molecules and the universe's evolution. The supercomputers now on TeraGrid have a combined peak performance of 4.5 trillion floating−point operations per second. The goal of the first phase is "to get a respectable computer infrastructure on the ground" and to work on software development, Pennington said. Each of the four main TeraGrid partner sites has had to adjust its software infrastructure for compatibility with the other partners.
Source: http://www.gcn.com/vol1_no1/daily−updates/24763−1.html

26. *January 27, eSecurityPlanet.com* — **Apple plugs Apache, app flaws. For the second time this month, Apple has released security patches to correct vulnerabilities found in several versions of its Mac OS X**. A "moderately critical" vulnerability in two Apache modules, mod_alias and mod_rewrite, could conceivably give a network user escalated privileges or let them launch a denial−of−service attack . Security officials also modified how the mod_cgid communicates with CGI script, saying it was not "handled properly." Apple also patched an unspecified vulnerability in the SystemConfiguration subsystem that allows network admins to change network settings and system configuration. Unspecified vulnerabilities were also found in the Mac OS X mail application, Safari Web browser, Windows file sharing and in the environment variables area. Earlier this month, Apple patched a lower−priority vulnerability in the code that allowed a local user to "crash" SecurityServer by inputting a long password into a keychain. Several applications in Mac OS X cannot operate without SecurityServer, causing a denial of service. **Fixes have been issued for Mac OS X versions: 10.3.2 client and server; 10.2.8 client and server; and 10.1.5 client and server and can be found at:**
http://www.secunia.com/advisories/10723/

Source: http://www.esecurityplanet.com/prodser/article.php/3304281

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 2 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_MYDOOM.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 6129 (dameware), 137 (netbios−ns), 1434 (ms−sql−m), 1433 (ms−sql−s), 4662 (eDonkey2000), 20168 (−−−), 445 (microsoft−ds), 80 (www), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *January 28, Press Enterprise (PA)* — **Police turn up more spraying gear, chemicals. Police searched Charles J. Lucarelli's apartment in McAdoo, PA Tuesday, January 27, and found more spraying devices and cans of paint thinner.** Lucarelli, 57, is scheduled for a hearing tomorrow, January 29, for outfitting his car as a mobile sprayer and causing a hazardous chemical and terrorism scare at a truck stop near Mifflinville January 11. Inside his apartment at 45 W. Blaine St., officers found Pennsylvania and New York road maps with several locations circled, police said. There were circles around Danville, Williamsport and Wilkes−Barre, said South Centre Township Police Chief Bill Richendrfer. Police also found sealed cans of paint thinner and a roll of plastic tubing, he said. Police confiscated the spraying devices, which seemed to be windshield washer pumps, but wrote down the name of the paint thinner and left the cans behind, Richendrfer said. The apartment was littered with court forms and lawsuit documents, he added. Lucarelli has a reputation as a frequent litigant. **Richendrfer said he was hoping to find a recipe or ingredient list for Lucarelli's chemical mixture because one substance remains unidentified. No such list was found.** The two chemical mixtures found in the car contained paint thinner, rubbing alcohol, gasoline and ammonia, he said.
Source: http://www.pe−online.com/283242832747842.bsp

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.